



U
S
A
N
E
T
A

TLA 7204VXR/7206VXR and 2900 XL Series Switch Implementation Guide

Distribution is limited to DoD Components for Administrative and Operational use. Requests for this document shall be referred to Director, U. S. Army Networks, Engineering, and Telecommunications Activity, ATTN: (AFSN-EN), Fort Huachuca, AZ 85613-5000

DIRECT SUPPORT ENGINEERING DIRECTORATE

**DEPARTMENT OF THE ARMY
U.S. ARMY NETWORKS, ENGINEERING,
AND TELECOMMUNICATIONS ACTIVITY
FORT HUACHUCA, ARIZONA, 85613-5000**

TLA 7204VXR/7206VXR and 2900 XL Series Switch Implementation Guide

DISTRIBUTION authorized to U.S. Government agencies and their
Administrative or Operational Use, August 2000. Requests for this document
be referred to Director, U.S. Army Networks, Engineering, and
Activitv. ATTN: (AFSN-EN). Fort Huachuca. AZ 85613-5000

DIRECT SUPPORT ENGINEERING DIRECTORATE U.S. ARMY NETWORKS, ENGINEERING, AND TELECOMMUNICATIONS ACTIVITY

_____/s/
RICHARD KELLETT
Computer Engineer, DSED

_____/s/
ROBERTO B. SUAREZ
Team Leader, Network
Operations Team

_____/s/
DENNIS M. ROBBINS
Chief, Network Systems
Division

_____/s/
MICHAEL D. BOMBA
Director, Direct Support
Engineering Directorate

TLA 7204VXR/7206VXR AND 2900 XL SERIES SWITCH IMPLEMENTATION GUIDE

1.0	INTRODUCTION	4
1.1	PURPOSE	4
1.2	BACKGROUND	4
1.3	IOS RECOMMENDATION	5
1.4	HARDWARE RECOMMENDATION	5
2.0	GENERAL SYSTEM REQUIREMENTS	8
3.0	EVALUATION BASIS	9
4.0	HARDWARE AND CONFIGURATION INFORMATION	9
4.1	HARDWARE INFORMATION	9
4.2	CONFIGURATION INFORMATION	13
5.0	ACRONYMS	13

TLA 7204VXR/7206VXR and 2900 XL Series Switch Implementation Guide

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to provide a guideline for implementing the Cisco 7204VXR/7206VXR routers and 2900 XL series switch in the Top-Level Architecture (TLA). This document will identify an IOS (Internetworking Operating System) that meets operational and management requirements for the TLA Security router, supply methods to determine components to purchase, and the basic hardware and software configuration.

1.2 Background

The TLA is the portion of the Army installation network that interfaces between the Army installation network and the Wide Area Networks (WAN). It provides the network gateway functions. It includes all network equipment from the Army DISN Router Program (ADRP) router to the WAN service providers' points of presence on the installation. The TLA Security router is the system that establishes the connection to any and all service points.

The original TLA Bill of Material (BOM) recommended a Cisco 7204 Router and a Cisco Catalyst 2820 Ethernet Switch. Cisco now offers a VXR model to the 7200 Router Series and advises against purchase of the basic 7204 model, since it is near the end of its life cycle. Also, the basic 7204 model provides only four input/output (I/O) slots, which is insufficient for some installations. Cisco's Catalyst 2820 switch has 24 10BaseT ports and slots for two high Speed I/O modules. It is also near the end of its life cycle and has limited configuration options.

In order to assure that current and new TLA requirements are supported, the equipment must be maintainable/serviceable by the vendor and must provide increased data handling capabilities. Migration to newer Cisco 7204/06VXR platforms and 2900XL switches is recommended. The implementation guidance contained in this document is based on evaluation performed on 7204/06VXR and 2900 XL series of equipment. Evaluation was performed by the United States Army Networks, Engineering, and Telecommunications Activity (USANETA) Direct Support Engineering Directorate (DSED) and the United States Army Information Systems Engineering Command (USAISEC) Technology Integration Center (TIC).

1.3. IOS Recommendations

The following provides recommended IOS for use on the Cisco 7204VXR, 7206VXR, and 2900 XL Series Switches.

IOS Recommendations

Routers:

Cisco 7200 12.1.1aT1 Enterprise/FW/IDS/IPSEC 56. The download image name is c7200-jo3s56i-mz.121-1a.T1.bin.

BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 12.0(5)T1, RELEASE SOFTWARE(fc1)

Switches:

IOS (tm) C2900XL Software (C2900XL-C3H2S-M), Version 12.0(5)XU, RELEASE SOFTWARE (fc1)

1.4 Hardware Recommendation

The following BOM identifies hardware/software that will meet general TLA system requirements. Two choices are offered as the Security Router platform and as the Ethernet Switch platform in order to provide flexible interface solutions for small and large-scale implementations. In general the 7206VXR is the recommended Security Router platform, and the Cisco 2924M-XL is the recommended Ethernet Switch platform. As lower cost alternatives, the Cisco 7204VXR Router and the Cisco 2912XL Switch, may be used if the following conditions are met:

- a. The typical Cisco 7204VXR router implementation employs two “low bandwidth” port adapters. In this configuration, no more than three high speed interfaces are used. If less than two of the low bandwidth port adapters are required, more than three high speed interfaces may be used as long as the per bus bandwidth point total of 600 is not exceeded. Refer to the Hardware Configuration section in the document for further Port Adapter Information.
- b. The Cisco 2912XL switch can be used if no more than twelve 10/100 ethernet ports are required, and if all connecting devices are within 100 meters of the switch.

The 7206VXR platform provides two additional slots for increased port density. The Cisco 2924M-XL switch provides 12 additional built-in 10/100 ethernet ports and two slots for optional interface modules (10/100BaseTX Ethernet, 100BaseFX Ethernet, 1000BaseX GigabitEthernet, and UTP/Singlemode/Multimode OC3 ATM) increasing the port density and cost over the 2912XL switch. Both VXR router models have the same processing/functional capability. Both 2900XL-switch models have the same processing/switching capabilities. The routers and switches are maintainable with current CONUS-Theater Network Operations and Security Center (C-TNOSC)/management tool capability and support Cisco’s IOS/command line capability.

1.4.1 Recommended TLA BOM

Table 1 contains the recommended Bill of Material (BOM) for the purchase of the Army Security Router and the Security Ethernet Switch. The specific quantities of the options to be purchased will need to be determined to customize the configuration to the respective implementation.

Table 1

<u>Equipment</u>	<u>Nomenclature</u>	<u>QTY</u>
<u>Cisco 7206VXR Router Components</u>		
Cisco 7206VXR Bundle with NPE-300 and I/O Controller with FE	CISCO7206VXR/300	1
Cisco 7200 AC Power Supply Option, 280W	PWR-7200	1
Cisco 7200 Dual AC Power Supply Option, 280W	PWR-7200/2	1
Power Cord,110V	CAB-AC	2
Cisco 7200 I/O PCMCIA Flash Memory, 20MB Option	MEM-I/O-FLC20M	2
Cisco 7200 Series IOS ENTERPRISE/FW/IDS IPSEC 56	S72AHL-12101aT1	1
Cisco IOS 7200 Series WAN Packet Protocols/Netflow License	FR-WPP72	1
Cisco IOS 7200 Series InterDomain Routing/Tag Switching Lic	FR-IR72	1
256MB Memory for NPE-300/NPE-225/NPE-175 in 7200 Series	MEM-SD-NPE-256MB	1
Auxiliary/Console Port Cable Kit	ACS-2500ASYN	1
Cisco 7206 SMARTnet Maintenance (3 yrs)	CON-SNT-7206	1
<u>Cisco Catalyst 2924M- XL Switch</u>		
Cisco 2924, 24-port 10/100 Ethernet Switch with two module slots (Enterprise Edition)	WS-C2924M-XL-EN	1
Power Cord,110V	Power Cord,110V	1
Catalyst 2900 SMARTnet Maintenance (3yrs)	CON-SNT-WS-C2924-XL	1
<u>WAN Cable Options</u>		
RS 530 Cable, DTE, Male – 10 Feet	CAB-530MT	
<u>I/O Port Adapter Options</u>		
1-Port Fast Ethernet 100BaseTx Port Adapter	PA-FE-TX	
1-Port Fast Ethernet 100BaseFx Port Adapter	PA-FE-FX	
4-Port Ethernet 10BaseT Port Adapter	PA-4E	
4 Port Serial Port Adapter, Enhanced	PA-4T+	
1-Port ATM Enhanced OC3c/STM1 Multimode Port Adapter	PA-A3-OC3MM	
1-Port ATM Enhanced OC3c/STM1 Singlemode(LR)Port Adapter	PA-A3-OC3SML	

1-Port ATM Enhanced OC3c/STM1
Singlemode(LR)Port Adapter

PA-A3-OC3SMI

1.4.2 Alternative TLA BOM

For some situations where there is a lesser connectivity requirement the 7204VXR may be used. Table 2 contains the recommended BOM for this configuration. The specific quantities of the options to be purchased will need to be determined to customize the configuration to the respective implementation.

Table 2

<u>Equipment</u>	<u>Nomenclature</u>	<u>QTY</u>
<u>Cisco 7204VXR Router Components</u>		
7204VXR System with single AC Power Supply	CISCO7204VXR	1
Cisco 7200 AC Power Supply Option	PWR-7200	1
Cisco 7200 Dual AC Power Supply Option, 280W	PWR-7200/2	1
Power Cord,110V	CAB-AC	2
7200VXR NPE-300 w/ 32MB base mem + 32 MB extra mem	NPE-300	1
Cisco 7200 Input/Output Controller with Fast Ethernet Port	C7200-I/O-FE	1
Cisco 7200 I/O PCMCIA Flash Memory, 20MB Option	MEM-I/O-FLC20M	2
Cisco 7200 Series IOS ENTERPRISE/FW/IDS IPSEC 56	S72AHL-12101aT1	1
Cisco IOS 7200 Series WAN Packet Protocols/Netflow License	FR-WPP72	1
Cisco IOS 7200 Series InterDomain Routing/Tag Switching Lic	FR-IR72	1
256MB Memory for NPE-300/NPE-225/NPE-175 in 7200 Series	MEM-SD-NPE-256MB	1
Auxiliary/Console Port Cable Kit	ACS-2500ASYN	1
Cisco 7204 SMARTnet Maintenance (3 yrs)	CON-SNT-7204	1
<u>Cisco Catalyst 2912 XL Switch</u>		
Cisco Catalyst 2912, 12-port 10/100 Switch (Enterprise Edition)	WS-C2912-XL-EN	1
Power Cord,110V	Power Cord,110V	1
Catalyst 2900 SMARTnet Maintenance (3yrs)	CON-SNT-WS-C2912-XL	1
<u>WAN Cable Options</u>		
RS 530 Cable, DTE, Male – 10 Feet	CAB-530MT	
<u>I/O Port Adapter Options</u>		
1-Port Fast Ethernet 100BaseTx Port Adapter	PA-FE-TX	
1-Port Fast Ethernet 100BaseFx Port Adapter	PA-FE-FX	
4-Port Ethernet 10BaseT Port Adapter	PA-4E	
4 Port Serial Port Adapter, Enhanced	PA-4T+	
1-Port ATM Enhanced OC3c/STM1 Multimode Port Adapter	PA-A3-OC3MM	
1-Port ATM Enhanced OC3c/STM1 Singlemode(LR)Port Adapter	PA-A3-OC3SML	

2.0 GENERAL SYSTEM REQUIREMENTS

The Department of the Army directed USASC to manage an Army-wide Intrusion Detection System (IDS) with a centralized worldwide monitoring view and to manage the Army access control lists on the associated Army Security Routers. In accomplishing this mission, USASC developed a standard installation Information Assurance (IA) architecture. The IA architecture is integrated with the Army common-user unclassified network Wide Area Network (WAN) gateway equipment into the installation standard network TLA.

The standard installation IA TLA consists of the following:

The C-TNOSC, previously known as the ANSOC, managed Army Security Router for terminating the WAN Internet Protocol (IP) circuit(s) coming on to the installation.

The C-TNOSC managed Security Ethernet Switch that provides an access point for monitoring of all IP traffic entering and exiting the installation from the Army Security Router.

The C-TNOSC managed Intrusion Detection System which is connected to the security Ethernet switch for monitoring all IP traffic entering and exiting the installation from the Army Security Router.

The DOIM managed ADRP/installation router/switch which is connected to the Security Ethernet Switch. It allows for application of any DOIM required access control lists and for distribution of the IP traffic to the installation data network.

The DOIM managed ADRP/installation terminal server with RADIUS-compliant identification and authentication for telephone dial-in data modem access to the installation IP network.

In order to meet the Department of the Army Network Security Improvement Program (NSIP) direction, all IP traffic entering or leaving the Army installation must go through the installation TLA equipment. It will be protected by the IA access control list filters on the Army Security Router and monitored by the IA Intrusion Detection System that is connected to the Security Ethernet Switch.

The recommended hardware/software must meet or exceed current and future TLA security stack requirements while focusing on equipment life cycle and maintenance considerations. The TLA system architecture types that must be supported by the recommended equipment are:

- a. Type 1 (Current) - Consists of 10Mbps data flow rate between Security and ADRP router with no Asynchronous Transfer Mode (ATM) WAN service
- b. Type 2 (Current) - Consists of 100Mbps data flow rate between Security and ADRP router with no ATM WAN service

- c. Type 3 (Current) - Consists of 100Mbps data flow rate between Security and ADRP router with ATM WAN service
- d. Type 4 (New) - Consists of 100Mbps data flow rate between Security and ADRP router with multiple high speed WAN interfaces(ATM/Fast Ethernet)
- e. Type 5 (Future) – Consists of Dual 100Mbps data flow rate between Security and ADRP router with multiple high speed WAN interfaces(ATM/Fast Ethernet)

3.0 EVALUATION BASIS

The recommendations detailed in this document are based upon evaluations performed during May through July, 2000. The evaluations performed under TR No. DSED00035 included the following areas:

- Configuration Commands/Syntax
- Out-of-Band Management
- SNMP Management using HP Openview, CiscoWorks, and NetHealth
(access control, traps, demand polls, statistics...)
- Network Timing Protocol
- Authentication Accounting Authorization (AAA) support using
RADIUS/TACACS+
- Telnet and traceroute sessions
- Interface Access Control Lists and debugging
- BGP, OSPF, and RIP protocols(distribution, debugging, Access Control Lists)
- Secondary IP addresses
- IP classless
- NetFlow
- Throughput, reliability (data loss), and router CPU utilization when the SUT is
utilized in standard and proposed TLA architectures.

4.0 HARDWARE AND CONFIGURATION INFORMATION

4.1 Hardware Configuration

4.1.1 Minimum revision level for the port adapters

Table 3

Port Adapter	Description	Minimum Revision Level
<i>PA-4E</i> <i>PA-8E</i>	Ethernet 10BaseT Port Adapters	1.14
<i>PA-5EFL</i>	5-Port Ethernet 10BaseFL Port Adapter	1.5

PA-H	HSSI Port Adapters	1.17
PA-2H	HSSI Port Adapters	1.3
PA-A3-T3 PA-A3-E3 PA-A3-OC3MM PA-A3-OC3SMI PA-A3-OC3SML	Enhanced ATM Port Adapters	2.0
PA-8T-V35	V.35 Port Adapters	1.13
PA-8T-232	EIA/TIA-232 Port Adapters	1.4
PA-8T-X21	X.21 Port Adapters	1.13

All other port adapters have no minimum revision level requirement. Any port adapters ordered with the 7206VXR systems will operate in a VXR chassis.

4.1.2 General Hardware Information

The front of the Cisco 7206/04 VXR router provides access to an input/output (I/O) controller and interface port adapters. The I/O controller has a local console port (for connecting a DTE device) and an auxiliary port (for connecting a DCE device) for configuring and managing the router; PCMCIA Card slots for Flash memory cards or Flash Disks; and an optional Fast Ethernet port. Figure 1 shows a Cisco 7206VXR with installed port adapters and an I/O controller with a Fast Ethernet port.

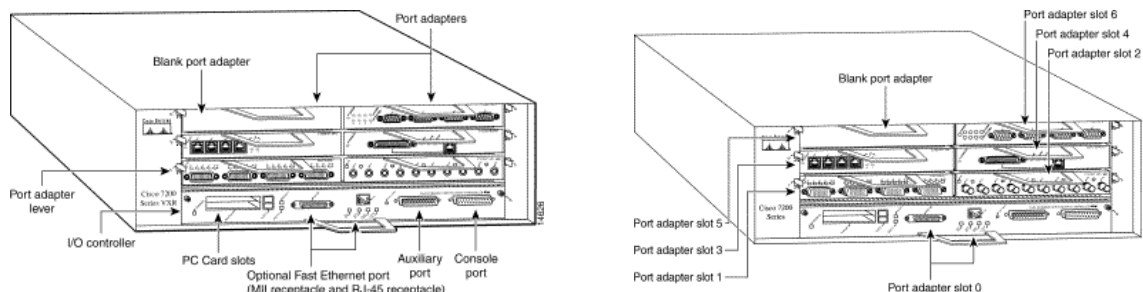


Figure 1: Cisco 7200 Series Router---Front View (Cisco 7206VXR Shown)

Note In Figure 1, a blank port adapter is installed in port adapter slot 5. To ensure adequate airflow across the router's internal components, ensure that each port adapter slot is filled with either a port adapter or a blank port adapter.

The rear of the Cisco 7206/04VXR router provides access to a network processing engine (NPE) and up to two 280W AC-input or DC-input power supplies (see Figure 2).

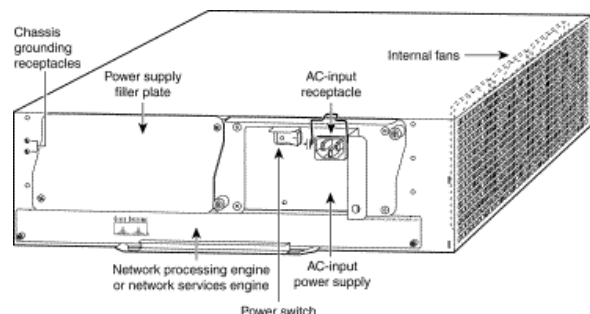


Figure 2: Cisco 7200 Series Router---Rear View

The NPE has no external connectors or LEDs. There is a handle for removing and installing the engines and two captive installation screws for securing them to the chassis. A fully configured Cisco 7206/04 VXR router operates with only one installed power supply; however, a second, optional power supply of the same type provides hot-swappable, load-sharing, redundant power. The power supply has the router's main power switch and an AC-input power receptacle. Adjacent to the power supply bays are two chassis grounding receptacles that provide a chassis ground connection for ESD equipment or a two-hole grounding lug (see Figure 2).

All port adapters and service adapters installed in Cisco 7206/04VXR routers connect to two Peripheral Component Interconnect (PCI) buses, mb1 and mb2, on the routers' midplane that provide a path to packet I/O memory and the system (routing and switching) processor. The Fast Ethernet port on the I/O controller connects to a third PCI bus, mb0 (through mb1), for packet routing and switching. In the Cisco 7206VXR router, bus mb1 is for the optional Fast Ethernet port on the I/O controller and port adapter slots 1, 3, and 5; bus mb2 is for port adapter slots 2, 4, and 6. (See figure 1 for slot numbering)

The Cisco 7206 router's bandwidth affects the port adapter distribution in the chassis, as well as the number and types of port adapters you can install. Port adapters should be evenly distributed by bandwidth between bus mb1 and bus mb2. Cisco 7206VXR routers that have an NPE-300 installed use bandwidth points to determine port adapter distribution and configuration. Bandwidth points are an assigned value related to bandwidth; however, the value is adjusted based on how efficiently the hardware uses the PCI bus.

Table 1 of the Cisco 7200 VXR Installation and Configuration Guide found at <http://www.cisco.com/univercd/cc/td/doc/product/core/7206/7206cfig/3471pac6.htm> lists adapter types, bandwidths or bandwidth points, and processor memory requirements. Some of the applicable entries include:

Port Adapter Type	Product Name	Bandwidth Points	Processor Memory Required
PA-A3-0C3SMI	Enhanced ATM	300	1.0Mb
PA-8E	8-port Ethernet 10BaseT	80	0.40 MB
PA-5EFL	5-port Ethernet 10BaseFL	50	0.25 MB
PA-4E	4-port Ethernet 10BaseT	40	0.25 MB
PA-FE-TX	1-port Fast Ethernet 100BaseTX	200	0.10 MB
PA-FE-FX	1-port Fast Ethernet 100BaseFX	200	0.10 MB
C7200-I/O-FE	1-port Fast Ethernet I/O controller	200	0.10 MB
PA-4T+	4-port synchronous serial,	0	0.20 MB

	enhanced		
--	----------	--	--

To ensure that the Cisco 7206VXR port adapter configuration is within the router operating limitations, observe the following guidelines (keeping in mind that the Fast Ethernet port on the I/O controller is considered a high-bandwidth port adapter):

For a Cisco 7206 VXR router with an NPE-300:

Keep the combined bandwidth point total of PCI bus mb1 (port adapter slot 0, slot 1, slot 3, and slot 5) to 600 or less.

Keep the combined bandwidth point total of PCI bus mb2 (port adapter slot 2, slot 4, and slot 6) to 600 or less.

If these guidelines are exceeded, one of the following error messages will be displayed:

%C7200-3-PACONFIG: Exceeds 600 bandwidth points for slots 0, 1, 3 & 5

%C7200-3-PACONFIG: Exceeds 600 bandwidth points for slots 2, 4 & 6

%C7200-3-PACONFIG: Exceeds 600 bandwidth points on both odd & even numbered slots

Note: To prevent anomalies from occurring while the router is in use, it is strongly recommended to restrict the port adapter types installed in the router according to the guidelines listed above.

4.2 General Configuration Information

When performing an initial configuration of a 7206VXR, there are some suggested points to consider. The variance of half- and full-duplex 100 Mbps Ethernet requires strict adherence. Although the 2900XL will auto-negotiate and will communicate between full duplex and half duplex connections, optimal performance will result when the 2900XL switch is connected using full duplex for all ports. The 2900XL will display errors to the console port which is symptomatic of the mismatched full and half duplex connections.

When long Access Control Lists are used, the 7206VXR performance will be increased with the use of NetFlow. The respective interface requires the **ip route-cache flow** command to be implemented. The NetFlow use can be monitored with the **show ip cache flow** command. Cisco document **Configuring NetFlow Switching** can be found at

www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt3/xcdnfc.htm

By default from the factory, the 2900XL is configured to a single VLAN consisting of all ports. The switch will have increased performance if it is configured with VLANs that consist only of ports which require connectivity. The users guide provides information to initiate a new VLAN and to configure the ports to be joined to the new VLAN.

For a port to monitor the traffic on or between any other ports, the port that is used to connect the monitoring device must be configured to perform this function. The User's guide provides information on the **port monitor** command.

Usage and syntax of the commands **vlan database**, **switchport mode access**, **switchport access vlan-id**, **port monitor**, **show vlan brief**, etc., can be found in:

Cisco IOS Commands

http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35sa6/cmdref/macrccli.htm

Usage and syntax of **vlan database**, **vlan vlan-id name vlan-name**, **show vlan name vlan-name**, etc. can be found in: Configuring VTP and Virtual LANs at

http://www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35sa6/eescg/mascvtp.htm-xtocid2203126

5.0 ACRONYMS

Table 4

ADRP	Army DISN Router Program
ANSOC	Army Network and Systems Operations Center
ATM	Asynchronous Transfer Mode
BOM	Bill of Materials
C-TNOSC	CONUS - Theater Network and Operations Security Center
CPU	Central Processing Unit
DCE	Data Communication Equipment
DIMM	Dual In-line Memory Module
DISN	Defense Information Systems Network
DOIM	Director of Information Management
DSED	Direct Support Engineering Directorate
DTE	Data Terminal Equipment
ESD	Electro-Static Discharge
I/O	Input/Output
IA	Information Assurance
IDS	Intrusion Detection System
IOS	Internetwork Operating System
IP	Internet Protocol
LED	Light Emitting Diode
MB	MegaByte
MHz	Mega Hertz
NIPRNET	Non-secure Internet Protocol Router Network
NSIP	Network Security Improvement Program
PCMCIA	Personal Card Memory Card International Association
RADIUS	Remote Authentication Dial-In User Server
ROM	Read Only Memory
SDRAM	Synchronous Dynamic Random Access Memory
TLA	Top Level Architecture
TR	Technical Report
USASC	US Army Signal Command

UTP	Unshielded Twisted Pair (copper wire)
WAN	Wide Area Network